

Serial No. 09/829,674
Page 8 of 12**REMARKS**

Applicant cancels claim 2. Claims 1 and 3-10 remain pending in the present application. Applicant amends claims 1 and 7-10 to incorporate the features of canceled claim 2, and amends claims 3-4 and 6 to depend from claim 1. Applicant refers to Figs. 1-2 and their corresponding description in the specification for exemplary embodiments of and support for the claimed invention. No new matter has been added.

Claims 1-6 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter of the invention. In particular, the Examiner, again, objected to the phrase "public/secret keys" in claim 1. Applicant has already amended claim 1 to recite "public and secret keys" by the Amendment filed on September 6, 2005. Applicant, again, respectfully requests that the Examiner withdraw the §112, ¶2 rejection.

Claim 10 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,373,950 to Rowney in view of "Handbook of Applied Cryptography" by Menezes et al.; claims 1-2 and 4-9 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Rowney in view of U.S. Patent No. 6,732,269 to Baskey et al. and further in view of Menezes et al.; and claim 3 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Rowney, Baskey et al., Menezes et al., and further in view of U.S. Patent No. 6,351,813 to Mooney et al. Applicant amends independent claims 1 and 7-10 to incorporate features of canceled claim 2 in a good faith effort to further clarify the invention as distinguished from the cited art, and, therefore, respectfully traverses the rejections.

84123996_1.DOC

Serial No. 09/829,674

Page 9 of 12

The Examiner cited a new portion of Menezes et al., p. 552, as alleged disclosure of the claimed feature of encrypting common key X using a common key X'. The newly-cited portion of Menezes et al. describes encrypting a key using another key. Applicant respectfully submits that the combination of references would still fail to teach the claimed feature of authenticating, by proxy, a direct communication between a user terminal and an electronic market server.

Again, the Examiner acknowledged that Rowney does not disclose "the proxy server being provided between a user terminal and an electronic market server and the shared key being a common key," (page 5, lines 17-19 of the Office Action) and relied upon Baskey et al. as a combining reference for disclosing a proxy server between a client and a server, and relied upon Menezes et al. as a further combining reference for disclosing a common key. The cited portions of Baskey et al., col. 5, lines 17-37, merely describe an SSL proxy server operable in routing client specific SSL connections onto a persistent secure connection between the SSL proxy server and a transaction server. And the cited portions of Menezes et al., provide overviews of symmetric-key encryption (also known as single-key, one-key, private key, and conventional encryption), and "key-encrypting keys."

Therefore, even assuming, arguendo, that it would be obvious to one skilled in the art to combine Rowney, Baskey et al., and Menezes et al., the combination would suggest, at most, a persistent secure connection between the SSL proxy server and a transaction server, as described in Baskey et al., through which communication from a user terminal is conducted. Such a combination would, thus, still fail to disclose or suggest, "an encrypted communication is executed directly between the user terminal and the electronic market server by using the

84125996_1.DOC

Serial No. 09/829,674

Page 10 of 12

common key X that was exchanged between the proxy server and the electronic market server," as claimed.

With respect to the features of canceled claim 2, the Examiner apparently relied upon col. 2, lines 35-38 and col. 15, lines 47-58 of Rowney, describing a user smart card and a payment gateway, respectively, as alleged disclosure of the claimed "home card." In particular, the Examiner contended that a user smart card inherently includes the claimed features. Applicant respectfully submits that the cited references do not disclose or suggest, at the time the claimed invention was made, that a user smart card inherently includes incorporating the features of the claimed home card to the claimed proxy/first server. As such, even assuming, arguendo, that it would be obvious to one skilled in the art to combine Rowney, Baskey et al., and Menezes et al., such combination would still fail to teach or suggest,

"[a] proxy server, provided between a user terminal and an electronic market server, including a proxy facility for executing authentication and encryption to the electronic market server, instead of the user terminal, in an electronic commercial transaction, comprising:

an establishing means for establishing an encrypted communication session between the user terminal and the proxy server, using public/ and secret keys of the user terminal and an electronic signature both transmitted from the user terminal;

a proxy means for executing authentication of a certificate and exchanging a common key X between the proxy server and the electronic market server, using public and secret keys of the electronic market server;

an informing means for informing the common key X to the user terminal through the encrypted communication session, which common key X is encrypted by using a common key X' that was exchanged between the user terminal and the proxy server; and

a home card including an encryption managing means for executing the electronic signature and authentication of the certificate in order to execute authentication and exchange of the common key to the electronic market server.

84125996_1 DOC

Serial No. 09/829,674

Page 11 of 12

whereby an encrypted communication is executed directly between the user terminal and the electronic market server by using the common key X that was exchanged between the proxy server and the electronic market server," as recited in claim 1.
(Emphasis added)

Accordingly, Applicant respectfully submits that independent claim 1, together with claims 4-6 dependent therefrom, is patentable over Rowney, Baskey et al., and Menezes et al. individually and in combination. Independent claims 7-10 incorporate features that correspond to those of claim 1 cited above, and are, therefore, patentable over the cited references for at least the same reasons.

With respect to dependent claim 3, the Examiner relied upon Mooney et al. to specifically address the additional features thereof. The cited portions of Mooney et al., col. 1, lines 59-67, col. 2, lines 1-11, and col. 9, lines 31-36, describe the use of a user smart card for access control, the use of a secret password for decrypting encrypted data transferred from a first site to a second site, and the use of a second password or biometric information to generate an encryption key. They do not teach or suggest the above recited features of claim 1. Applicant, therefore, respectfully submits that the combination of Mooney et al. with Rowney, Baskey et al., and Menezes et al. would not teach or suggest the above features of claim 1 that are incorporated in dependent claim 3, even assuming such a combination would have been obvious to one skilled in the art. Accordingly, Applicant submits that claim 3 is patentable over Rowney, Baskey et al., Menezes et al., and Mooney et al. for at least the above-stated reasons with respect to claim 1, from which it depends.

Statements appearing above in respect to the disclosures in the cited references represent the present opinions of the undersigned attorney and, in the event that the Examiner disagrees

84125996_1.DOC

Serial No. 09/829,674

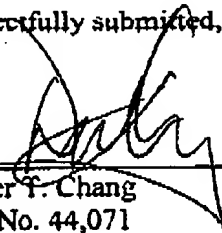
Page 12 of 12

with any of such opinions, it is respectfully requested that the Examiner specifically indicate those portions of the respective reference providing the basis for a contrary view.

In view of the remarks set forth above, this application is in condition for allowance which action is respectfully requested. However, if for any reason the Examiner should consider this application not to be in condition for allowance, the Examiner is respectfully requested to telephone the undersigned attorney at the number listed below prior to issuing a further Action.

Any fee due with this paper may be charged to Deposit Account No. 50-1290.

Respectfully submitted,



Dexter F. Chang
Reg. No. 44,071

CUSTOMER NUMBER 026304
Telephone: (212) 940-6384
Fax: (212) 940-8986 or 8987
Docket No.: 100794-11683 (FUJA 18.570)
DTC:fd

84125996_1.DOC